Background – Presenter

- Senior IT Auditor with Pennsylvania’s State System of Higher Education for 7 years
- Master’s degree in Information Systems
- Undergraduate degree in Accounting
- Three certifications: CPA, CISA, and CISSP
- Worked 15+ years in the banking and healthcare industries as an auditor, information security manager, and research manager
Background – State System

- Pennsylvania’s State System of Higher Education was established by statute on July 1, 1983.
- The State System is comprised of 14 universities and a Chancellor’s office.
- The State System serves more than 110,000 students, making it the largest provider of higher education in Pennsylvania.
- It also employs more than 12,000 faculty and staff, making it one of the largest employers in the Commonwealth.
The Office of Internal Audit and Risk Assessment (OIARA) was established in 2009. The OIARA derives its operating authority through a Board of Governors’ policy under the direction of a Board Audit Committee. OIARA is a small audit shop of 7 individuals. Each year, the OIARA minimally completes 2 audits for each university. OIARA mainly performs 4 types of audits: compliance, operational, financial, and information technology.
Audit Constraints

• Limited auditing resources
• 15 information technology departments across the State System
• 5,000+ systems and devices
Our Problem

So how does the OIARA provide an effective information technology auditing function to the State System?
Our Solution

The OIARA decided to perform a high level review of each information technology department.
The following presentation provides the State System’s OIARA’s interpretation and application for conducting an Information Technology General Control Review.

Presentation material is based upon relevant information technology review practices and is tailored to the State System and is provided for illustrative purposes only.

The State System’s internal audit process is revised as additional information becomes available. Participants should reference and consult any additional materials and resources deemed appropriate, in formulating their own process for conducting and evaluating information technology controls within their individual operating environments.

The State System does not claim rights, ownership, or precision of information contained within this presentation. The opinion expressed is that of the presenter.
Project Engagement

• Governance and Management Frameworks
• Information Technology Risk Management
• Scope, Objectives and Methodology
• Key Controls, Findings, and Analysis
• Remediation of Control Weaknesses
Governance and Management Frameworks

The OIARA conducted its review based primarily upon the principles and guidance promulgated from the following five widely accepted governance and management frameworks supporting information technology operations.

• COSO: Internal Control – Integrated Framework
• COBIT 5: A Business Framework for the Governance and Management of Enterprise IT
• ISO 20000:2011: IT Service Management System
• ISO 22301:2012: Business Continuity Management System
• ISO 27001:2013: Information Security Management System
Good IT governance enables an organization to take full advantage of its information, thereby maximizing benefits, capitalizing on opportunities, and gaining competitive advantage.

Each entity within the State System is responsible to establish and maintain a viable governance structure for accountability and trust regarding IT operations.
Management of information technology risks is a key component of IT governance.

Each entity within the State System is responsible to establish and maintain a systematic process for assessing and treating its information technology risks.
IT Risk Management

The risk assessment process should include the following activities:

• Identify critical information assets
• Valuate the identified assets, taking into account the identified legal and business requirements and the impacts resulting from a loss of confidentiality, integrity, and availability
• Identify significant threats and vulnerabilities for the identified assets
• Assess the likelihood of the threats and vulnerabilities to occur
• Calculate the risk
• Evaluate the risks against a predefined risk scale
IT Risk Management

Once a risk has been assessed, a business decision needs to be made as to how the risk is to be treated.

For all those risks where the option to reduce the risk has been chosen, appropriate controls should be implemented to reduce the risks to the level that has been identified as acceptable, or at least as much as is feasible toward that level.

Once the risk treatment decisions have been made, activities to implement these decisions need to be identified and planned.
IT Risk Management

Risk treatment plans should include these activities:

• Identification of limiting factors and dependencies
• Establishment of priorities
• Agreement of milestones and deadlines
• Identification of requirements and resources
• Approvals to spend or allocate resources
Scope, Objectives, and Methodology

As part of its annual work plan, the OIARA performed over a four-year period (2010-14) an IT General Control Review at each of the 14 State System universities and the Office of the Chancellor.

The purpose of this high-level review was to identify significant risks and potential control weaknesses within the State System’s IT control environment.
Scope, Objectives, and Methodology

The review involved meetings and table top discussions with management and the completion of an Information Systems and Technology Questionnaire.

This comprehensive exercise consisted of 470 questions and examined internal control measures within 15 different IT-related areas.
Information System & Technology Questionnaire

• Pennsylvania State Employee Credit Union
• Bank Examiners
Information System & Technology Questionnaire

• Obtained from National Credit Union Administration's website (www.ncua.gov)
• Modified to fit the State System's environment
• Identifies major risks and assesses the adequacy of the IT control environment
• Is a comprehensive tool that examines 15 IT-related areas
Information System & Technology Questionnaire

- Authentication
- Business Continuity Planning
- Firewalls
- IDS & IPS
- IT Policies
- Networks
- Penetration Test
- Remote Access

- Routers
- Security Program
- Servers
- Vendor Oversight
- Virus Protection
- Website
- Wireless
In 2013, NCUA updated the Information System & Technology Questionnaire. It is now called the IT Exam Questionnaire.

The IT Exam Questionnaire contains expanded sections for physical and environmental controls and virtualization.
Authentication

Through discussion and observation, the auditor should review and evaluate the entity's authentication strategy and techniques, i.e., user authentication, user controls, biometric devices, encryption keys, digital signatures, monitoring and reporting, and fraud and identity theft.
Authentication

• Is there a password policy which address length and type of characters, frequency of password change, reuse of previous passwords, etc.?
• Does the computer system lock out an employee after a number of failed log-on attempts?
• Is employee access changed when a user's duties change and removed promptly upon leaving employment? Is this monitored and reviewed?
• Has management implemented adequate procedures to ensure the proper identification of a user before resetting or reissuing a password?
• Does the university have in place an awareness program to educate users against fraud and identity theft?
Authentication

Assessment of internal controls governing user authentication frequently identifies the lack of one or a combination of the following controls:

• Assessing the adequacy of employed authentication methods
• Establishing a formalized user management process
• Strengthening logical access controls (e.g., complex passwords, account lockouts)
Business Continuity Planning

Through discussion and observation, the auditor should review and evaluate the adequacy of the entity's business continuity plan in the event of a service outage, disaster, or point of failure along service delivery channels, i.e., business continuity planning process, physical security, backup and recovery, backup power, and incident response.
Business Continuity Planning

• Does the university have a business continuity plan?
• Has the university performed a business impact analysis?
• Has management established appropriate backup policies and procedures to ensure the timely restoration of critical services?
• Does the university have adequate uninterruptible power supply protection to perform an orderly systems shutdown in case of power loss?
• Is the business continuity plan periodically tested?
Business Continuity Planning

Common areas where information technology controls may not be sufficient include the lack of one or a combination of the following controls:

- Identifying mission-critical processes and systems
- Conducting a business impact analysis
- Developing and maintaining comprehensive business continuity program
- Enhancing IT infrastructure redundancy
- Performing regular recovery testing
Firewall Security and Administration

Through discussion and observation, the auditor should review and evaluate the firewall environment to determine if the design is adequate to support the network infrastructure, i.e., firewall policy, operations, third-party vendors, and audit logs and monitoring.
Firewall Security and Administration

- Who is responsible for managing the firewall?
- Who has access to the firewall?
- Are there rule change procedures, which include approval process, documentation retention, and verification process?
- How often are the configurations (e.g., rules, ports, etc.) reviewed? Who is responsible for the review, and how is the review documentation retained?
- Are automated alerts in place (e.g., rule changes)?
Firewall Security and Administration

Assessment of internal controls governing firewall security and administration may commonly identify the lack of one or a combination of the following controls:

- Conducting regular security reviews
- Ensuring proper change management (e.g., software updates, rules)
- Hardening firewall security
- Monitoring audit logs
- Performing system backups and recovery tests
Intrusion Detection & Prevention Systems

Through discussion and observation, the auditor should review and evaluate the intrusion detection and prevention system to determine if it is adequately securing the entity’s network environment from potentially harmful network activities, i.e., intrusion detection and prevention policies, operation, detection logs and reports, change management, signature updates, and testing.
Intrusion Detection & Prevention Systems

• Does the university have an intrusion detection and prevention system?
• Does the system notify management of intrusions in real time?
• Does the intrusion detection system maintain an adequate list of attack signatures?
• Do intrusion detection policies and procedures address escalation procedures?
• Are intrusion detection logs and reports regularly reviewed and any necessary action taken?
Intrusion Detection & Prevention Systems

Appropriate intrusion detection and prevention systems controls are vital in safeguarding electronic information. Key points to consider in this regard include internal controls ensuring:

• Implementing and maintaining an intrusion detection and prevention system
• Developing and enhancing event notification and escalation procedures
IT Policies

Through discussion and observation, the auditor should review and identify the entity’s policies, procedures, practices, and controls over the IT environment, i.e., acceptable use, data classification, incident response, and information security policies.
IT Policies

Does the university minimally have the following policies?

• Acceptable use
• Data classification
• Information handling
• Incident response
• Physical security
• Record retention
Information technology policies and procedures outline an organization’s process for management and handling of specific matters dealing with the overall internal control environment necessary to ensure the safeguarding and maintenance of electronic information, i.e., its confidentiality, integrity, and availability.

The completion of an IT internal control review may typically identify the lack of IT policies and procedures, or necessary enhancements in the development and formalizing of IT policies and procedures.
Network Security and Administration

Through discussion and observation, the auditor should review and evaluate the resources and accountability associated with an entity’s network infrastructure, i.e., network access controls, network architecture and design, change management, patch management, software development, and network monitoring.
Network Security and Administration

- Has the administrator account been renamed to a strong user name?
- Are policies, procedures, and practices in place describing how the network components are configured to ensure adequate security?
- Does the university have written change management procedures that address management approval, scheduled upgrades, testing, and implementation?
- Does management use a formal methodology or process to guide the acquisition, development, or maintenance of new or modified software?
- Is the physical access to computer facilities adequately controlled?
- Is the computer room climate adequately controlled?
Network Security and Administration

Typical internal control deficiencies associated with network security and administration may frequently identify the lack of one or a combination of the following controls:

• Developing and formalizing the change management process
• Enhancing physical security
• Formalizing the project management process
• Hardening network security
• Limiting the use of a generic administrator account
• Monitoring audit logs
• Performing IT resource and capacity planning activities
Penetration Tests

Through discussion and observation, the auditor should review and evaluate the penetration test process and results, i.e., penetration test agreements, test reports, and their scope.
Penetration Tests

• Does the university perform any penetration testing for its mission critical systems?
• Does the penetration test agreement indicate that all compromised systems, if applicable, are restored to their initial configurations, if possible, and all files, tools, and other data left behind by the exercise are removed to the greatest extent possible?
• Did the firm engaged to perform the penetration test present management with a written report documenting the results of the test?
• Did management take timely action to address the weaknesses identified in the report?
Penetration Tests

To ensure the integrity and security of an organization’s information technology platform:

• Regular penetration tests and vulnerability assessments should be completed.
• Outcomes of testing should be reviewed with leadership, identifying those areas where internal controls are not sufficient to ensure improper access to the organization’s technology systems and information.
Remote Access

Through discussion and observation, the auditor should review and evaluate the entity's remote access technologies policies and practices, i.e., remote access processes.
Remote Access

- Are there policies and procedures in place which describe the authorization, authentication, and monitoring of remote access users, such as employees, students, and vendors?
- Is remote access monitored?
- Does management approve and review remote access permissions initially and at least annually thereafter?
- Does management employ the proper procedures to detect and deny unauthorized remote access?
Remote Access

The availability of ensuring remote access to campus staff, faculty, and students continues to become an expected service and commonplace within university operations. Assessment of safeguards regarding remote access may typically identify deficiencies including the lack of one or a combination of the following controls:

• Establishing a formalized user management process
• Monitoring vendor access
Router Security and Administration

Through discussion and observation, the auditor should review and evaluate if management practices related to entity’s router operations are adequate, i.e., security and administration.
Router Security and Administration

- Does documentation (e.g., topology maps) exist to identify the routers that exist on the university’s network?
- Is physical access to the routers controlled?
- Has training been provided to individuals responsible for router support and maintenance?
- Is the router configuration reviewed regularly?
- Are all unneeded services shut down on the routers?
Router Security and Administration

Assessment outcomes may typically identify opportunities to improve internal controls addressing the lack of one or a combination of the following safeguards:

- Hardening router security
- Monitoring audit logs
- Conducting regular security reviews
- Performing system backups and recovery tests
Security Program

Through discussion and observation, the auditor should review and evaluate the entity’s information security program to determine if the entity and its data are adequately protected, i.e., security management processes, security awareness, monitoring, and system auditing.
Security Program

• Has management developed and implemented a comprehensive security policy and program, which describe the standards and procedures used to protect IT assets and university data?

• Has the ability to administer information security and alter system security parameters been limited to appropriate personnel?

• Does the university have policies and procedures in place to address incidents and events?

• Are security monitoring reports regularly generated and reviewed?

• Is a security awareness program in place?

• Is a security awareness program in place?
Assessment of internal controls evaluating the effectiveness of a security program may typically identify opportunities for improvements addressing one or a combination of the following controls:

- Establishing an information security management system
- Assessing information technology risks
- Improving incident response plans and processes
- Monitoring system security
- Providing security awareness, education, and training
Through discussion and observation, the auditor should review and evaluate management practices related to an entity’s servers to determine if they are adequate to support the network infrastructure, i.e., service infrastructure, administrative controls, and server security.
Server Security and Administration

- Is there a list of the hardware, software and operating system for each server in service?
- Are any of the servers in a DMZ?
- Is the responsibility for patch management assigned to a specific person?
- Have the servers been hardened?
- Is there documentation on the vulnerability scans performed and actions taken to address the identified vulnerabilities?
- Are server audit logs monitored and reviewed for irregularities?
- Are there procedures for backing up the operating system and software for each server?
Server Security and Administration

Key elements to ensure are in existence regarding server security and administration may typically include:

• Implementing a DMZ
• Hardening server security
• Monitoring audit logs
• Performing system backups and recovery tests
Vendor Oversight and Management

Through discussion and observation, the auditor should review and evaluate the entity’s vendor due diligence oversight program, i.e., technology, security and continuity assessment process, contract maintenance, and service level agreements.
Vendor Oversight and Management

- Did the university request and evaluate the service provider’s financial condition initially and then annually thereafter?
- Did the university obtain adequate information detailing the security measures in place to protect the facility, data, etc.?
- Did the university review the service provider’s business resumption contingency plans to ensure that any services considered mission critical for the organization can be restored within an acceptable timeframe?
- Does the contract address minimum service levels for each service provided by the vendor?
- Does the university regularly review reports documenting vendor’s performance?
Vendor Oversight and Management

Assessment and evaluation associated with vendor management internal safeguards may frequently identify the lack of one or a combination of the following controls:

• Developing standardized contract language
• Conducting financial condition reviews
• Performing security and continuity assessments
• Reviewing service level and performance agreements
Virus Protection

Through discussion and observation, the auditor should review and evaluate the entity's malware policies, procedures, and practices, i.e., virus protection, spyware, spam filtering, and pop-up blockers.
Virus Protection

- Is the virus protection software on each critical server connected to the network?
- Is the virus protection software on each personal computer connected to the network?
- Are the virus protection pattern files updated on a regular basis?
- Does the university periodically verify that the automated scheduler is performing the updates?
Virus Protection

Within the IT environment virus protection is typically well executed and addressed through the deployment of vendor developed virus protection software.

In assessing virus protection, it is important to consider and evaluate access points for virus penetration that could adversely impact technology operations and effectiveness of the virus protection software.

Typical internal control deficiencies identified through an assessment of virus protection controls may detect failure in maintaining current and updated versions of virus protection software.
Website Administration

Through discussion and observation, the auditor should review and evaluate the entity's operation of its website and management practices, i.e., website administration, design and content control, and applications.
Website Administration

• Is there a statement on the type of information which is permissible on the university’s website?
• How are changes made to the website?
• Are website changes approved by management and is documentation retained showing approved changes?
• If applications are electronically accepted by the university, is this process secure?
Website Administration

Assessment of internal controls governing website administration may typically identify opportunities for improvement or strengthening of controls related to centralized approval processes ensuring the style, accuracy, linkage, and relevance of information contained within an entity’s website.
Wireless Security and Administration

Through discussion and observation, the auditor should review and evaluate the adequacy of controls over wireless local area networks, i.e., security, administration, monitoring, and validation.
Wireless Security and Administration

- Are wireless equipment and security devices included in the topology for the university network infrastructure?
- Have key employees received appropriate training regarding network, application, and security controls?
- Has the wireless network been hardened and secured?
- Does the university regularly review access point logs?
- Are independent security assessments obtained to determine if the university is adhering to internal policies and industry best practices for wireless networks?
Wireless Security and Administration

The current atmosphere exists supporting the desire to provide wireless connectivity to vast groups of individuals interacting within a campus environment.

With this goal of providing wireless availability, an important safeguard is conducting regular security reviews of the wireless structure to ensure effective application, accompanied with necessary internal controls governing usage and access.
Finding Remediation

When internal audits of information technology internal controls identify improvement opportunities or specific deficiencies, it is vital to perform follow-up assessments evaluating the effectiveness of corrective remediation efforts.

The OIARA maintains a formalized process to evaluate prior internal audit report recommendations and implementation of the auditee’s management responses necessary to remediate engagement findings.

Specifically with regard to information technology control matters, some corrective measures expressed by auditees contain timelines and are budgetary dependent.
Questions?

Office of Internal Audit and Risk Assessment

David L. Shissler, CPA, CISA, CISSP
DSHISSLER@PASSHE.EDU
Phone: (717) 720-4245